IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

SAIT KURMANGALIYEV, on behalf of himself and all others similarly situated, Plaintiff, v. PARKMOBILE, LLC, Defendant.	)	Case No. **CLASS ACTION COMPLAINT**

Plaintiff Sait Kurmangaliyev ("Plaintiff"), by its undersigned counsel, files this Class Action Complaint on behalf of itself and a class of all similarly situated persons against Defendant ParkMobile, LLC ("ParkMobile" or "Defendant"). Plaintiff bases the forgoing allegations upon personal information and belief, the investigation of counsel, and state the following:

INTRODUCTION

1. ParkMobile is an application that launched in 2008 for smart phones and devices that helps users find and pay for parking over their device and, additionally, offers parking reservations for in communities and for events, including concerts, sporting events, airport parking, and campus parking. ParkMobile claims

it is "committed to creating tech-based solutions that power smart mobility and make parking hassles of the past obsolete."

2. ParkMobile operates in cities and states throughout the country, including 8 of the top 10 largest cities in the United States. In all, ParkMobile provides parking services for 557 different cities and venues in 42 States. These include, but are not limited to, New York City, San Francisco, Washington D.C., Denver, Kansas City, Boston, Oakland, Nashville, Chicago, Milwaukee, Baltimore, and Atlanta.

3. To assist users in providing its services, ParkMobile collects a variety of sensitive data, including names, license plate numbers, email addresses, phone numbers, vehicle nicknames, passwords, and home addresses. This type of personal and sensitive data is highly targeted by hackers who seek to exploit that data for nefarious purposes. In the wrong hands, these types of sensitive and personally identifying information may be wielded to cause significant harm to the user's whose information was stolen.

4. ParkMobile assures users that it is highly sophisticated tech company and a technology innovator. It assured users that it can keep their information safe and uses industry standard data security measures. Contrary to its representations and promises, however, ParkMobile utilized inadequate data security measures it

knew, or should have known, put the sensitive data it solicited, collected, and stored at significant risk of theft by or exposure to nefarious parties.

5. Consequently, sometime in or around March 2021, hackers breached ParkMobile's data environment and accessed the sensitive user data that it solicited, collected and stored, and had promised to secure ("Data Breach").

6. Initially, ParkMobile represented that no data had been stolen in the Data Breach. On April 12, 2021, however, KrebsOnSecurity, an online security blog, reported that nefarious parties were selling sensitive data on 21 million ParkMobile customers. The data reportedly included customer email addresses, dates of birth, phone numbers, license plate numbers, hashed passwords, and mailing addresses. Gemini Advisory, a sophisticated threat intelligence firm confirmed KrebsOnSecurity's report.

7. On April 13, 2021—after KrebsOnSecurity had publicly reported the Data Breach had exposed sensitive data—ParkMobile acknowledged that sensitive had indeed been stolen in its Data Breach and recommended but, unusually, did not require users change their passwords.

8. ParkMobile attempted to downplay the Data Breach, claiming only "basic" user data was stolen, claiming no credit card data had been compromised and only encrypted passwords had been stolen. The reality, however, is that the

supposedly "basic" information stolen from ParkMobile is highly valuable and can be used to cause great harm to ParkMobile's users.

9. KrebsOnSecurity reported that the ParkMobile data was being sold for an "insanely high" price. Understandably so, the types of data stolen from ParkMobile can be used to facilitate a host of fraudulent activity, causing harm to ParkMobile's users.

10. Plaintiff Sait Kurmangaliyev used ParkNYC, ParkMobile's application for parking in New York City. ParkNYC is owned and operated by ParkMobile and, like ParkMobile, was impacted by the Data Breach. Sait received a notice from Credit Karma that his information was exposed in ParkMobile's Data Breach. Around the same time, Plaintiff noticed an increase in spam directed towards him. Plaintiff remains at a continued risk of harm due to the exposure and potential misuse of his personal data by criminal hackers.

11. As such, Plaintiff brings this Complaint on behalf of persons who's personally identifying information and other sensitive data was stolen during the Data Breach. Plaintiff asserts claims for negligence, negligence per se, and for declaratory and injunctive relief.

PARTIES

12. Plaintiff Sait Kurmangaliyev is a resident of Brooklyn, New York. He used ParkMobile's parking application for New York City, called ParkNYC. He received a notice that his information was exposed during the Data Breach. Plaintiff's information was included in the batch of information on 21 million ParkMobile users for sale on the dark web. After the Data Breach, Kurmangaliyev noticed an increase in spam calls.

13. Defendant ParkMobile, LLC owns and operates the ParkMobile parking application for smart phones and devices. Defendant ParkMobile, LLC is a Delaware Limited Liability Company with its principal place of business at 1100 Spring Street NW, Atlanta, Georgia. Defendant is a citizen of Georgia. The sole member of Defendant ParkMobile, LLC is ParkMobile USA, Inc. Member ParkMobile USA, Inc. is a Delaware corporation with its principal place of business at 1100 Spring Street NW, Atlanta, Georgia. ParkMobile USA, Inc. is a citizen of Georgia.

JURISDICTION AND VENUE

14. This Court has subject matter jurisdiction over this case pursuant to 28 U.S.C. § 1332(d), the Class Action Fairness Act, which affords federal courts with original jurisdiction over cases where any member of the plaintiff class is a citizen

of a state different from any defendant, and where the amount in controversy exceeds $5,000,000, exclusive of interest and costs. Here, Plaintiff is diverse from Defendant because Plaintiff resides in New York and ParkMobile resides in Georgia, where it and its sole member are headquartered. Plaintiff alleges that, in the aggregate, the claims of all purported class members exceed $5,000,000, exclusive of interest and costs.

15. Defendant is a Delaware LLC with its principal place of business in Atlanta, Georgia. Defendant is a citizen of Georgia. Its sole member, ParkMobile USA, Inc. is also a citizen of Georgia. Plaintiff is a citizen of New York. Minimal diversity requirement under CAFA is met.

16. This Court has general personal jurisdiction over Defendant because Defendant and its sole member are citizens of the State of Georgia, are headquartered and operate their principal place of business in Atlanta, Georgia. Defendant has minimum contacts with Georgia because it is located there and conducts substantial business there, and Plaintiffs' claims arise from ParkMobile's conduct in Georgia.

17. This Court is the proper venue for this case pursuant to 28 U.S.C. § 1391(a) and (b) because Defendant and its sole member reside in this District, a substantial part of the events and omissions giving rise to Plaintiff's claims occurred

in Georgia and because ParkMobile conducts a substantial part of its business within this District.

BACKGROUND

A. ParkMobile Collects Sensitive Information from Users.

18. ParkMobile is an application for smart devices, phones, and computers that provide parking-related services. ParkMobile claims to "help[] millions of people easily find an pay for parking on their mobile devices" and help users "to quickly pay for street and garage parking without having to use a meter or kiosk."[1] Additionally, ParkMobile providers parking reservations for concerns, sporting events, airports, campuses and other venues.[2]

19. ParkMobile operates in at least 42 different states and provides parking-related services for over 550 venues, including 450 cities throughout the United States. ParkMobile's state-specific applications may have different names. For example, ParkMobile developed and fully operated the ParkNYC application, which provides ParkMobile's parking services to New York City users. However, in effect, the ParkNYC application is the same as ParkMobile.

---

[1] *About ParkMobile*, ParkMobile.io (last visited Jun. 28, 2021), https://parkmobile.io/company/

[2] *Id.*

20. ParkMobile claims its "Mission" is to "make parking easier" by "creating tech-based solutions that power smart mobility and make parking hassles of the past obsolete."[3] ParkMobile further states its "innovative solutions . . . eliminate friction while maximizing convenience and efficiency."[4]

21. ParkMobile represents itself as a trusted leader in technology and smart applications, calling itself a "Vanguard" of travel and technology. It claims its team members have "a wide range of experience in everything from software development to commercial real estate" which "better connect[s] the practicalities of parking with tech-based solutions that make it hassle free."[5]

22. It further represents that its team is made up of "Smart People" who "Build[] Smart Solutions" and "[p]erson by person, [it] has put together an awesome team that does great work and has a great time doing it."[6]

23. ParkMobile represents that its core values include "a healthy obsession with the customer experience" and "[f]rom [its] app and online tools to [its] customer service team . . . [it] make[s] every interaction with ParkMobile and [its] products,

---

[3] *Id.*

[4] *Id.*

[5] *Id.*

[6] *Careers*, ParkMobile.io (last visited Jun. 28, 2021), https://parkmobile.io/company/careers/

perfect." It claims to hold itself to "a higher standard" and expresses that it "own[s] [its] commitments and are accountable."

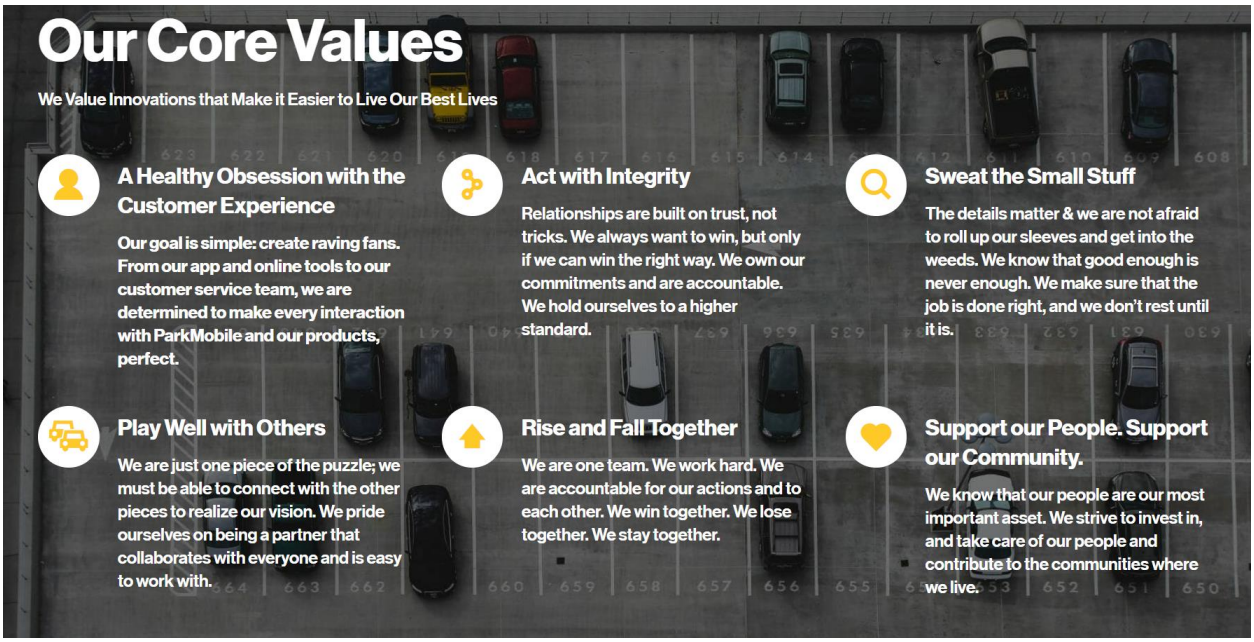

Image 1. A picture of ParkMobile's description of its "Core Values"

24. In providing its parking-related service to users, ParkMobile collects sensitive user data. For example, ParkMobile collects users' names, license plate numbers, email addresses, phone numbers, vehicle nicknames, passwords, and home addresses. Additionally, ParkMobile collects and retains information on users' locations. ParkMobile recognized the importance of protecting this data. For instance, in 2012, it wrote: "There are numerous methods by which hackers may

steal information . . . and the entry of personal data is at risk at any time depending on [one's] physical surroundings and the security of [one's] network or device."[7]

25. ParkMobile assures users, however, that their sensitive data is safe with ParkMobile. For example, ParkMobile's "Member Services" promised users that "ParkMobile utilizes industry standard encryption methods to ensure cardholder details (name, credit card number, etc.) are stored using strong encryption algorithms."[8] ParkMobile further claims it "has been audited to ensure that [its] cardholder capture, handling, encryption, and storage are all compliant with industry methods."[9] ParkMobile also represents that it uses "trusted methods to ensure cardholder data is protected[.]"

26. Instead, ParkMobile warns that the real risk is not the theft of information from it, but rather, from the users themselves: "While Parkmobile utilizes trusted methods to ensure cardholder data is protected, it is outside the scope of the Parkmobile security to ensure that a customer computer or mobile phone is

[7] Member Services, *Is my account and credit card information safe?*, ParkMobile.io (Feb. 21, 2012), https://support.parkmobile.io/hc/en-us/articles/203299650-Is-my-account-and-credit-card-information-safe-

[8] *Id.*

[9] *Id.*

not compromised."[10] ParkMobile then claims that there are many ways in which users' data may be stolen from their own devices.

27. As it turns out, ParkMobile was wrong. The real risk was not from its users, but from ParkMobile. On March 26, 2021, ParkMobile disclosed it had been the subject of a "cybersecurity incident" and "launched an investigation" in response.[11]

B. ParkMobile's Inadequate Data Security Measures Exposed Users' Sensitive Data

28. After the Data Breach, ParkMobile admitted it had identified a "vulnerability in a third-party software that [it] use[d]." Initially, however, ParkMobile claimed that "no sensitive data or Payment Card Information . . . was affected."[12]

29. As the investigation progressed, ParkMobile learned that sensitive data had indeed been exposed. Less than three weeks after its initial notice, ParkMobile admitted that its "investigation has confirmed that basic user information—license plate numbers . . . email addresses and/or phone numbers, and vehicle nicknames—

---

[10] *Id.*

[11] *Update: Security Notification – March 2021*, ParkMobile.io (last visited Jun. 28, 2021), https://support.parkmobile.io/hc/en-us/articles/360058639032-Update-Security-Notification-March-2021

[12] *Id.* described in the section titled "Previous Notification from March 26, 2021").

[were] accessed."[13] ParkMobile also disclosed that mailing addresses may have been affected. ParkNYC issued the same notice on the data breach, noting that ParkMobile, the developer of the ParkNYC app, became aware of a cybersecurity incident linked to a vulnerability in a third-party software."[14]

30. ParkMobile's second notification may have been prompted by a KrebsOnSecurity article that identified a batch of data for sale on the dark web that included information on 21 million ParkMobile's users.[15] KrebsOnSecurity reported that the stolen data included customer email addresses, dates of birth, phone numbers, license plate numbers, hashed passwords and mailing addresses.[16] Gemini Advisory, a sophisticated threat intelligence company based in New York, confirmed KrebsOnSecurity's report on batch of data for sale on the dark web.[17] The stolen data was available for sale at an "insanely high price."[18]

---

[13] *Id.* (described in the section titled "Previous Notification from April 13, 2021").

[14] *ParkNYC Security Notice*, ParkNYC.zendesk.com (last visited Jun. 28, 2021), https://parknyc.zendesk.com/hc/en-us/articles/360060887852

[15] Brian Krebs, *ParkMobile Breach Exposes License Plate Data, Mobile Numbers of 21M Users*, KrebsOnSecurity (Apr. 12, 2021), https://krebsonsecurity.com/2021/04/parkmobile-breach-exposes-license-plate-data-mobile-numbers-of-21m-users/

[16] *Id.*

[17] *Id.*

[18] *Id.*

31. ParkMobile acknowledged that, after the Data Breach, it needed to take measures to enhance its cybersecurity. For example, in its March 26, 2021 notice, ParkMobile noted that it had: "taken additional precautionary steps since learning of the incident, including eliminating the third-party vulnerability, maintaining our security, and continuing to monitor our systems."[19] Furthermore, although it claimed to have taken "extensive measures to protect user passwords," ParkMobile recommended that users change their passwords and provided instructions to do so because "encrypted passwords were accessed[.]"[20] KrebsOnSecurity noted, however, that it was unusual that ParkMobile was not requiring users to change their passwords given that those passwords had been stolen.[21]

32. Nearly a month after the Data Breach, ParkMobile reported it needed to continue to take efforts to "maintain [its] security and monitor [its] systems."[22]

C. ParkMobile Knew It Needed to Protect Users' Sensitive Data

33. As a technology leader providing cloud-based services, ParkMobile knew, or should have known, that it needed to implement measures to adequately

[19] *Id.* (described in the section titled "Previous Notification from March 26, 2021").

[20] *Id.* (described in the section titled "Update: April 15, 2021").

[21] Krebs, *supra* note 15.

[22] Update: Security Notification, *supra* note 11 (described in the section titled "Previous Notification from April 15, 2021").

protect sensitive data. Indeed, ParkMobile consistently represented that it technologically sophisticated and a leader in technological innovation.

34. Additionally, in its notices on the Data Breach, ParkMobile acknowledged it was bound to implement certain, basic security measures to protect passwords and payment card data. In fact, as far back as 2012, ParkMobile wrote that it "is a PCI Level 1 Vendor" meaning it had to "ensure that our cardholder capture, handling, encryption and storage [were] all compliant with industry methods."[23]

35. Other sources have also provided warnings to companies like ParkMobile of the need to protect sensitive data.

36. For example, the FTC has also issued numerous guidelines for businesses highlighting the importance of reasonable data security practices. The FTC notes the need to factor data security into all business decision-making.[24] According to the FTC, data security requires: (1) encrypting information stored on computer networks; (2) retaining payment card information only as long as

[23] *See* Member Services, *supra* note 7.

[24] Federal Trade Comm'n, *Start with Security A Guide For Business, Lessons Learned from FTC Cases* (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

necessary; (3) properly disposing of personal information that is no longer needed; (4) limiting administrative access to business systems; using industry tested and accepted security methods; (5) monitoring activity on networks to uncover unapproved activity; (6) verifying that privacy and security features function properly; (7) testing for common vulnerabilities; and (8) updating and patching third-party software.[25]

37. The FTC treats the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5(a) of the FTC Act.

38. As such, the FTC has issued orders against businesses that failed to employ reasonable measures to secure sensitive payment card data. *See In the matter of Lookout Services, Inc.*, No. C-4326, ⁋ 7 (June 15, 2011) ("[Defendant] allowed users to bypass authentication procedures" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks, such as employing an intrusion detection system and monitoring system logs."); *In the matter of DSW, Inc.*, No. C-4157, ⁋ 7 (Mar. 7, 2006) ("[Defendant] failed to employ sufficient

[25] *Id.*; Federal Trade Comm'n, *Protecting Personal Information, A Guide For Business* (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

measures to detect unauthorized access."); *In the matter of The TJX Cos., Inc.*, No. C-4227 (Jul. 29, 2008) ("[R]espondent stored . . . personal information obtained to verify checks and process unreceipted returns in clear text on its in-store and corporate networks[,]" "did not require network administrators . . . to use different passwords to access different programs, computers, and networks[,]" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks . . ."); *In the matter of Dave & Buster's Inc.*, No. C-4291 (May 20, 2010) ("[Defendant] failed to monitor and filter outbound traffic from its networks to identify and block export of sensitive personal information without authorization" and "failed to use readily available security measures to limit access between instore networks . . ."). These orders, which all proceeded ParkMobile's Data Breach, further clarify the measures businesses must take to meet their data security obligations.

D. ParkMobile's Data Breach Harmed Plaintiff and the Class

39. Plaintiff's and the Class's data exposed in the Data Breach constitute the type of data specifically targeted by and valuable to hackers.

40. Indeed, hackers increasingly sell these sensitive records on the black market to purchasers who seek to use the personally identifying information to create

fake IDs, make fraudulent transactions, obtain loans or commit other acts of identity theft.[26]

41. The risk of identity theft after a data breach is lasting. The U.S. Government Accountability Office's research into the effects of data breaches found that "in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data has been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot rule out the significant risk of future harm."[27]

42. Plaintiff used and provided information to ParkNYC, ParkMobile's application for its users in New York City. ParkNYC solicited sensitive information from Plaintiff, including his name, license plate number, email address, mailing address, and other information. Plaintiff provided the information ParkNYC requested.

---

[26] *How do hackers make money from your stolen data?*, Emsisoft.com (Feb. 20, 2020), https://blog.emsisoft.com/en/35541/how-do-hackers-make-money-from-your-stolen-data/

[27] Report to Congressional Requesters, Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown 29 (Jun. 2007), http://www.gao.gov/new.items/d07737.pdf (last accessed Nov. 30, 2018).

43. Around March 2021, Plaintiff received a notice from Credit Karma stating: "In March 2021, ParkMobile's database was allegedly breached. Even if you don't use your ParkMobile account anymore, it's important to protect any info that was exposed." Credit Karma further warns that Plaintiff's data, including, but not limited to, his name, date of birth, email address, password and phone number, were exposed.

44. Plaintiff and the Class, having had their data exposed by ParkMobile, face a continued risk that their sensitive data will be used for a nefarious purpose, causing them harm. Plaintiff already reported seeing a noticeable increase in spam shortly after the Data Breach, making it likely that the increase in spam is a direct result of the theft of Plaintiff's data from ParkMobile.

CLASS ALLEGATIONS

45. Plaintiff brings this action on behalf of himself and all other similarly situated Class members pursuant to Rule 23(a), (b)(2) and (b)(3) of the Federal Rules of Civil Procedure and seek certification of the following Nationwide Class:

> All individuals that received or were otherwise sent notice that their data was potentially compromised due to ParkMobile's Data Breach.

46. Excluded from the class is ParkMobile and its subsidiaries and affiliates; all employees of ParkMobile; all persons who make a timely election to

be excluded from the class; government entities; and the judge to whom this case is assigned and his/her immediate family and court staff.

47. Plaintiff reserves the right to, after conducting discovery, modify, expand or amend the above Class definition or to seek certification of a class or subclasses defined differently than above before any court determines whether certification is appropriate.

48. **Numerosity**. Consistent with Rule 23(a)(1), the members of the Class are so numerous and geographically dispersed that joinder of all Class members is impracticable. Plaintiff believes that there are hundreds of thousands of members of the Class. The number of reportedly impacted individuals already exceeds 100,000, and Plaintiff believes additional entities and persons may have been affected by the Data Breach. The precise number of class members, however, is unknown to Plaintiff. Class members may be identified through objective means. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

49. **Commonality and Predominance**. Consistent with Fed. R. Civ. P. 23(a)(2) and with 23(b)(3)'s commonality and predominance requirements, this action involves common questions of law and fact which predominate over any

questions affecting individual Class members. These common questions include, without limitation:

a. Whether ParkMobile knew or should have known that its data environment and cybersecurity measures created a risk of a data breach;

b. Whether ParkMobile controlled and took responsibility for protecting Plaintiff's and the Class's data when solicited that data, collected it, and stored it on its servers;

c. Whether ParkMobile's security measures were reasonable in light of the FTC data security recommendations, state laws and guidelines, industry standards, and common recommendations made by data security experts;

d. Whether ParkMobile owed Plaintiff and the Class a duty to implement reasonable security measures;

e. Whether ParkMobile's failure to adequately secure Plaintiff's and the Class's data constitutes a breach of its duty to institute reasonable security measures;

f. Whether ParkMobile's failure to implement reasonable data security measures allowed the breach of its data systems to occur and caused the theft of Plaintiff's and the Class's data;

g. Whether reasonable security measures known and recommended by the data security community could have prevented the breach;

h. Whether Plaintiff and the Class were injured and suffered damages or other losses because of ParkMobile's failure to reasonably protect its data systems; and

i. Whether Plaintiff and the Class are entitled to relief.

50. **Typicality**. Consistent with Fed. R. Civ. P. 23(a)(3), Plaintiff is a typical member of the Class. Plaintiff and the Class are each persons whose provided data to ParkMobile, whose data resided on ParkMobile's servers, and whose personally identifying information was exposed in ParkMobile's Data Breach. Plaintiff's injuries are similar to other class members and Plaintiff seeks relief consistent with the relief due to the Class.

51. **Adequacy**. Consistent with Fed. R. Civ. P. 23(a)(4), Plaintiff is an adequate representative of the Class because Plaintiff is a member of the Class and is committed to pursuing this matter against ParkMobile to obtain relief for himself and for the Class. Plaintiff has no conflicts of interest with the Class. Plaintiff has also retained counsel competent and experienced in complex class action litigation of this type, having previously litigated data breach cases. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

52. **Superiority**. Consistent with Fed. R. Civ. P 23(b)(3), class action litigation is superior to any other available means for the fair and efficient adjudication of this controversy. Individual litigation by each Class member would strain the court system because of the numerous members of the Class. Individual litigation creates the potential for inconsistent or contradictory judgments and

increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court. A class action would also permit customers to recover even if their damages are small as compared to the burden and expense of litigation, a quintessential purpose of the class action mechanism.

53. **Injunctive and Declaratory Relief**. Consistent with Fed. R. Civ. P. 23(b)(2), Defendant, through its uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the class as a whole.

LEGAL CLAIMS

COUNT I
Negligence

54. Plaintiff repeats and re-alleges the allegations contained in every preceding paragraph as if fully set forth herein.

55. ParkMobile owed a duty to Plaintiff and the members of the Class to take reasonable care in managing and protecting the sensitive data it solicited from Plaintiffs and the Class, and managed and stored. This duty arises from multiple sources.

56. ParkMobile owed a common law duty to Plaintiff and the Class to implement reasonable data security measures because it was foreseeable that hackers would target ParkMobile's data systems and servers containing Plaintiff's and the Class's sensitive data and that, should a breach occur, Plaintiff and the Class would be harmed. ParkMobile alone controlled its technology, infrastructure, and cybersecurity. It further knew or should have known that if hackers breached its data systems, they would extract sensitive data and inflict injury upon Plaintiff and the Class. Furthermore, ParkMobile knew or should have known that if hackers accessed the sensitive data, the responsibility for remediating and mitigating the consequences of the breach would largely fall on individual persons whose data was impacted and stolen. Therefore, the Data Breach, and the harm it caused Plaintiff and the Class, was the foreseeable consequence of ParkMobile's unsecured, unreasonable data security measures.

57. Additionally, Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, required ParkMobile to take reasonable measures to protect Plaintiff's and the Class's sensitive data and is a further source of ParkMobile's duty to Plaintiff and the Class. Section 5 prohibits unfair practices in or affecting commerce, including, as interpreted and enforced by the FTC, the unfair act or practice by businesses like ParkMobile of failing to use reasonable measures

to protect sensitive data. ParkMobile, therefore, was required and obligated to take reasonable measures to protect data it possessed, held, or otherwise used. The FTC publications and data security breach orders described herein further form the basis of ParkMobile's duty to adequately protect sensitive information. By failing to implement reasonable data security measures, ParkMobile acted in violation of § 5 of the FTCA.

58. ParkMobile is obligated to perform its business operations in accordance with industry standards. Industry standards are another source of duty and obligations requiring ParkMobile to exercise reasonable care with respect to Plaintiff and the Class by implementing reasonable data security measures that do not create a foreseeable risk of harm to Plaintiff and the Class.

59. Finally, ParkMobile assumed the duty to protect users' sensitive data by soliciting, collecting, and storing users' data and, additionally, by representing to consumers that it would keep their data safe.

60. ParkMobile breached its duty to Plaintiff and the Class by implementing unreasonable data security measures that it knew or should have known could cause a Data Breach. As a self-proclaimed technology "Vanguard", ParkMobile knew or should have known that hackers might target sensitive data that ParkMobile solicited and collected on its users and, therefore, needed to use

reasonable data security measures to protect against a Data Breach. Indeed, ParkMobile acknowledged it was subject to certain standards to protect cardholder data and password information and utilize other industry standard data security measures. ParkMobile, furthermore, represented to users that their data was safe with ParkMobile.

61. ParkMobile was fully capable of preventing the Data Breach. ParkMobile, as a smart technology expert, knew or should have known of data security measures required or recommended by the FTC, state laws and guidelines, and other data security experts which, if implemented, would have prevented the Data Breach from occurring at all, or limited and shortened the scope of the Data Breach. ParkMobile thus failed to take reasonable measures to secure its system, leaving it vulnerable to a breach.

62. As a direct and proximate result of ParkMobile's negligence, Plaintiff and the Class have suffered and will continue to suffer injury, including the ongoing risk that their data will be used nefariously against them or for fraudulent purposes.

COUNT II
Negligence *Per Se*

63. Plaintiff repeats and re-alleges the allegations contained in every preceding paragraph as if fully set forth herein.

64. ParkMobile's unreasonable data security measures and failure to timely notify Plaintiff and the Class of the Data Breach violates Section 5 of the FTC Act. Although the FTC Act does not create a private right of action, both require businesses to institute reasonable data security measures and breach notification procedures, which ParkMobile failed to do.

65. Section 5 of the FTCA, 15 U.S.C. §45, prohibits "unfair. . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by businesses like ParkMobile of failing to use reasonable measures to protect users' sensitive data. The FTC publications and orders described above also form the basis of ParkMobile's duty.[28]

66. ParkMobile violated Section 5 of the FTC Act by failing to use reasonable measures to protect users' personally identifying information and sensitive data and by not complying with applicable industry standards. ParkMobile's conduct was particularly unreasonable given the sensitive nature and amount of data it stored on its users and the foreseeable consequences of a Data Breach should ParkMobile fail to secure its systems.

[28] *See supra*, note 75 (listing orders).

67. ParkMobile's violation of Section 5 of the FTC Act constitutes negligence per se.

68. Plaintiff and the Class are within the class of persons Section 5 of the FTCA (and similar state statutes) was intended to protect. Additionally, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. The FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same type of harm suffered by Plaintiff and the Class.

69. As a direct and proximate result of ParkMobile's negligence per se, Plaintiff and the Class have suffered and continue to suffer injury.

COUNT III

Declaratory and Injunctive Relief

70. Plaintiff repeats and re-alleges the foregoing allegations as if fully set forth herein.

71. Under the Declaratory Judgment Act, 28 U.S.C. §§2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority

to restrain acts, such as those alleged herein, which are tortious and which violate the terms of the federal and state statutes described above.

72. An actual controversy has arisen in the wake of the Data Breach at issue regarding Defendant's common law and other duties to act reasonably with respect to safeguarding the data of Plaintiff and the Class. Plaintiff alleges ParkMobile's actions in this respect were inadequate and unreasonable and, upon information and belief, remain inadequate and unreasonable. Additionally, Plaintiff and the Class continue to suffer injury due to the continued and ongoing threat of additional fraud against them or on their accounts.

73. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. ParkMobile owed, and continues to owe a legal duty to secure the sensitive information with which it is entrusted, specifically including information it obtains from its customers, and to notify impacted individuals of the Data Breach under the common law, Section 5 of the FTC Act;

b. ParkMobile breached, and continues to breach, its legal duty by failing to employ reasonable measures to secure its customers' personal information; and,

c. ParkMobile's breach of its legal duty continues to cause harm to Plaintiff and the Class.

74. The Court should also issue corresponding injunctive relief requiring ParkMobile to employ adequate security protocols consistent with industry standards to protect its users' (*i.e.* Plaintiff's and the Class's) data.

75. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another breach of ParkMobile's data systems. If another breach of ParkMobile's data systems occurs, Plaintiff and the Class will not have an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages, while warranted to compensate Plaintiff and the Class for their out-of-pocket and other damages that are legally quantifiable and provable, do not cover the full extent of injuries suffered by Plaintiff and the Class, which include monetary damages that are not legally quantifiable or provable.

76. The hardship to Plaintiff and the Class if an injunction does not issue exceeds the hardship to ParkMobile if an injunction is issued.

77. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another

data breach, thus eliminating the injuries that would result to Plaintiff, the Class, and the public at large.

PRAYER FOR RELIEF

78. Wherefore, Plaintiff, on behalf of himself and the Class, requests that this Court award relief as follows:

a. An order certifying the class and designating Plaintiff as the Class Representative and their counsel as Class Counsel;

b. An award to Plaintiff and the proposed Class members of damages with pre-judgment and post-judgment interest;

c. A declaratory judgment in favor of Plaintiff and the Class;

d. Injunctive relief to Plaintiff and the Class;

e. An award of attorneys' fees and costs as allowed by law; and

f. An award such other and further relief as the Court may deem necessary or appropriate.

JURY TRIAL DEMANDED

79. Plaintiff hereby demands a jury trial for all the claims so triable.

Respectfully submitted,

Dated: July 8, 2021

/s/ *MaryBeth V. Gibson*
MaryBeth V. Gibson
THE FINLEY FIRM, P.C.
3535 Piedmont Road
Building 14, Suite 230
Atlanta, GA 30305
Telephone: (404) 320-9979
Facsimile (404) 320-9978
mgibson@thefinleyfirm.com

Brian C. Gudmundson (*pro hac vice forthcoming*)
Michael J. Laird (*pro hac vice forthcoming*)
Rachel K. Tack (*pro hac vice forthcoming*)
ZIMMERMAN REED LLP
1100 IDS Center
80 South 8th Street
Minneapolis, MN 55402
Telephone: (612) 341-0400
Facsimile: (612) 341-0844
brian.gudmundson@zimmreed.com
michael.laird@zimmreed.com
rachel.tack@zimmreed.com

Bryan L. Bleichner *(pro hac vice forthcoming)*
CHESTNUT CAMBRONNE, PA
100 Washington Ave. S., Suite 1700
Minneapolis, MN 55401
Telephone: (612) 339-7300
bbleichner@chestnutcambronne.com